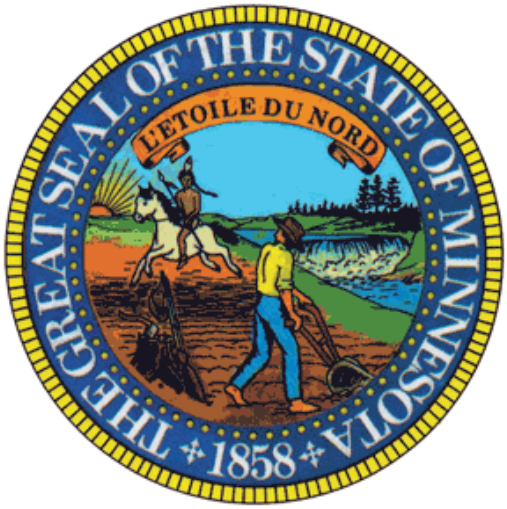
State of Minnesota



Enterprise Office of Technology (OET)

Glossary Of Information Security Terms And Definitions

Enterprise Security Office (ESO) Guideline

Version 1.01

Enterprise Chief Information Security Officer

Table of Contents

1.0 Guideline Statement

This glossary is used as the set of definitions for information security terms through out the Enterprise Security Office's (ESO) Enterprise Security Program. These terms will be used across all documents policies, standards, guidelines, processes, and reporting related to the Enterprise Security Program, but is a guideline for entities to use to cross-reference their own terms.

1.1 Reason for Guideline

While the Information Security industry uses common terms, which have generally accepted and understood meanings, subtitle inconsistencies and variations do occur. In order to ensure consistency and promote understanding, not only within the ESO, but also across the Agencies, this document captures the key terms and their definitions used throughout the Enterprise Security Program.

1.2 Applicability and Exclusions

These terms must be used across all documentation related to the Enterprise Security Program. This includes policies, standards, process documentation, and reporting coming from the Enterprise Security Office.

All government entities create documentation related to or reporting for the Enterprise Security Program must also use these definitions.

This document is offered as guidance to local government, higher education, K-12 or other government related entities for programs that are not related to the Enterprise Security Program.

1.3 Related Information

Minnesota Statutes 16E Office of Enterprise Technology

1.4 Forms and Instructions

Changes and additions maybe submitted to the Enterprise Security Office for consideration. All submissions must include the term, its definition, and two examples to provide clarity of the definition used.

2.0 Roles & Responsibilities

2.1 Enterprise Security Office

- Maintain this document
- Provide for peer review of terms and definitions through the vetting process of Enterprise Security Program documentation and reporting
- Maintain consistency across Enterprise Security Program documentation to these terms and definitions

2.2 Government Entity

- Align terms within agency documentation and reporting related to the Enterprise Security program to these terms and definitions
- Assist in peer review of terms and definitions through vetting process of the Enterprise Security Program documentation (e.g., policies, standards, etc.)

3.0 Directory of Acronyms

Acronym	Definition
ACL	Access Control List
ACS	Access Control Services
AES	Advanced Encryption Standard
BCM	Business Continuity Management
BIA	Business Impact Analysis
CA	Certificate Authority
CIA	Confidentiality, Integrity and Availability
CISO	Chief Information Security Officer
CMP	Crisis Management Plan
COOP	Continuity of Operations Plan
CSP	Credential Service Provider
DMZ	Demilitarized Zone
DNS	Domain Naming Service
DRP	Disaster Recovery Plan
EDI	Electronic Data Interchange
EVMS	Enterprise Vulnerability Management System
HIDS	Host Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host Intrusion Prevention System
ICMP	Internet Control Message Protocol
IMP	Incident Management Plan
IP	Internet Protocol
IRC	Internet Relay Chat
ITIL	Information Technology Infrastructure Library
L2TP	**L**ayer Two (**2**) **T**unneling **P**rotocol,
LAN	Local Area Network
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol

Acronym	Definition
LEAP	Lightweight Extensible Access Protocol
MAC	Mandatory Access Control
MAN	Metro Area Network
NAT	Network Address Translation
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OSI	Open System Interconnection
OS or O/S	Operating System
OST	Operational Support Team
PCI	Payment Card Industry
PEAP	Protected Extended Application Protocol
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QOS	Quality of Service
RA	Registration Authority
RADIUS	Remote Authentication Dial In User Service
RBAC	Role Based Access Control
RPO	Recovery Point Objective
RSA	Rivest Shamir Adelman
RTO	Recovery Time Objective
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SIH	Security Intelligence Hub
SME	Subject Matter Expert
SQL	Structured Query Language
SSL	Secure Sockets Layer
TBAC	Task-Based Access Control

Acronym	Definition
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/internet Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UID	Unique Identifier
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
VTMT	Vulnerability and Threat Management Team
WAN	Wireless Area Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

4.0 Glossary of Terms

A

TERM	DEFINITION
Access Control	A protective measure that prevents unauthorized access and ensures authorized access to physical or logical assets.
Access Control List (ACL)	The sum total of permissions or access controls on a given resource used to determine *authorization* of individuals, or other resources, to use it.
Access Rights	The cumulative privileges that are granted to a user, application, system, network, or other object that are necessary to perform one or more functions.
Account	A record of information that is used to uniquely define someone or something. **See Also:** *UserID*
Account Owner	The person that is accountable for the activities related to an *account*.
Administrator	
Agency, *-ies*	See *Government Entity*
Alert	The notification of a situation that may require a response. **Example**: An elevated status of readiness, such as putting a vendor or recovery team on alert to an evolving situation but not yet enacting full services. **Example**: An automatically triggered alert that is a notification of an attempted logon of a disabled account.
All Hazards Approach	An approach to continuity planning not based on specific interruption scenarios. A plan developed using this approach will be effective regardless of the incident.
Alternate Site	A location, other than normal facility, used to process data and/or conduct critical business functions in the event of a disaster. **Similar Terms:** Alternate Location, Alternate Processing Facility, Alternate Office Facility, Alternate Communication Facility, Recovery Center, Warm Site, Hot Site, Cold Site.
Application	Software that functions and is operated by means of computers

TERM	DEFINITION
	with the purpose of supporting the user's work.
Application Recovery	The component of disaster recovery that deals specifically with the recovery of business system software and data, occurs after the processing platform has been restored or replaced.
Archive	The data and records of a system or an organization that warrants continued preservation because of its value or other long term purpose.
Assessment	A process for identifying gaps in a given set of requirements by reviewing current state and desired state, resulting in a gap analysis report and recommendations for remediation. **See Also:** *Risk Assessment, Security Assessment*
Asset(s)	An asset is something of value to the state. Assets can be logical or physical in nature and can be classified as information (paper or electronic), systems, software, hardware, or people. **Example:** Paper healthcare records; the mainframe system **See Also:** *Information Asset*
Asset Criticality	The importance of an asset to a government entity as it relates to the entities mission and the asset's value.
Assumptions	The statements of a situation that are accepted to be true.
Audit	A process conducted by qualified, independent auditors to review and examine records and activities to verify compliance with applicable requirements resulting in a formal report that could require corrective action. **Example:** *Security Audit* of the controls for the PeopleSoft system.
Authenticate (-tion)	To verify the identity or origin of someone or something when the identity is presented/requested against an *authoritative source* of *authentication information*.
Authentication Information	The minimum information necessary to verify the identify or origin of someone or something.
Authentication Mechanism	A tool that is use to *authenticate* someone or something based on the given *authentication information*.
Authoritative Source	A source of information that has a creditable level of assurance to deem it reliable and correct.
Authorize (-d) (-ation)	Possessing official permission or being granted / denied approval by an *authoritative source* (e.g., owner, steward,

TERM	DEFINITION
	automated mechanism) to perform an action or set of activities. **Example:** A web application authorizes a user to access a function based on an access control policy. **Example:** An official management decision given by a senior agency official to allow the operation of an information system and to explicitly accept the risk to agency operations, assets, and individuals.
Authorized User	A person that possess the authority to perform an action or set of activities.
Availability	Ensuring the timely and reliable access to and use of data by authorized individuals, and the ability of a resource to perform its function at any given moment over a period of time.

B

TERM	DEFINITION
Backup	Copies of files, programs, data, etc. that facilitate recovery should the originals become corrupt or destroyed.
Baselines	The minimum level of security requirements necessary for an organization, *system*, *information asset*, etc.
Biometrics	A measurable, physical characteristic or personal behavioral trait by a human being that is used to recognize the *identity*, or verify the claimed *identity*, for *authentication* purposes. **Example:** Facial images, fingerprints, handwriting samples, etc.
Bot	An automated software program that operates as an agent for a user or another program, or simulates a human activity when it receives a specific input (like a ro-"bot").
Botnet	A group of computers that have the same *bot* installed, that can communicate with and control each other, and are usually used for malicious activities (create and send spam email, propagate malicious software, or other cyber attack).
Broad Remote Access	Individual and devices that have remote access to State resources which is equivalent to the user's access while on a government entity's internal, secure network (e.g., IPSec VPN, SSL VPN).
Business Continuation	A program covering disaster recovery and business resumption planning as well as prevention. **Similar Terms**: Continuity of Operations Planning

TERM	DEFINITION
Business Continuation Planning (BCP)	The process of documenting prevention measures, disaster recovery, business resumption and restoration plans. **Similar terms:** Business Continuity Planning, Business Resumption Planning, Continuity of Operations Planning and Disaster Recovery Planning.
Business Impact Analysis (BIA):	The process of analyzing an organization's business to determine the impact of a loss or disruption of service.
Business Interruption	Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations.
Business Interruption Costs	The costs or unrecoverable lost revenues associated with an interruption in normal business operations.
Business Recovery Critical Path	The order in which recovery processes are executed during a recovery effort. There are major milestones along the path, which are followed regardless of the organization.
Business Unit Recovery	The component of a business continuation plan which deals specifically with the relocation of key personnel in the event of a disaster and the provision of essential resources in order to perform their time-sensitive functions.

C

TERM	DEFINITION
Central Authority	**Example:**
Central Log Management System	A system which allows the central collection of system event messages (i.e., system logs) from various computing devices.
Certificate (-s)	A document attesting to the truth of certain stated facts. **See Also:** *Digital Certificate*
Certification Authority (CA)	A trusted entity in a public key infrastructure that is responsible for issuing and revoking certificates.
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.
Cipher	An algorithm used to *encrypt* or *decrypt* information.

TERM	DEFINITION
Ciphertext	Information in its encrypted form. More specifically, the data output from the *Cipher* or the input to the Inverse *Cipher*.
Cleartext	Information that is transmitted or stored in a form that is readily comprehensible, i.e. that has not been, nor is intended to be, *encrypted*. Similar to *plaintext* but differing in usage, with *cleartext* having connotation of the intentional non-encryption of information . **Example:** The message is being transmitted in cleartext
Client	An application or *information system* that accesses a remote service on another system (known as a *host* or *server*). Clients may additionally be labeled in other ways, such as by how much local processing they do (fat client, thin client), what hardware/software architecture they utilize ("Wintel"), or the services they subscribe to (web client, email client). **Example:** windows client, email client, web client
Cold Site	An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the critical business functions of an organization. Cold-sites have many variations depending on their communication facilities, UPS systems or mobility. **Similar terms:** Shell-site
Compensating Controls	Safeguards or countermeasures use to mitigate the severity or impact of an identified risk. Compensating controls can be technical or non-technical (e.g. process, policy, standards or procedures) in nature **Example:** The encryption of data on mobile devices **Example:** An HR policy on appropriate usages of State assets
Computerized Information Resources	Electronic data, applications, and technology.
Computing Device(s)	Any device that can autonomously perform some form of transaction with data that it receives, generates, stores, transmits, or deletes.

TERM	DEFINITION
	See Also: *Client, Host, Server* **Example:** Laptop, desktop, mainframe, cellular phone, etc.
Confidentiality	Preserving authorized restrictions on information access and disclosure.
Continuity of Operations Plan(ing) (COOP)	Series of plans used to respond, recover, resume and restore from a business interruption. **Similar Terms:** *Business Continuity Planning*
Controls	*Countermeasures* that are used to reduce the impact or probability of an identified *risk, or to* detect the event of or impact if an identified risk does occur. Controls can be detective or preventative in nature with automated or manual policies, procedures, or activities incorporated into a process, system, or environment. **Example:** *separation of duties* to limit risk of fraud in processes; audit logs to record and track activities; cameras, locked doors, fire suppression to protect physical assets
Countermeasures	Preventative (proactive or reactive) actions, devices, procedures, techniques, or other measures that reduce the impact of a vulnerability or the likelihood of successful exploitation of a vulnerability. **Similar Terms:** *Controls*, *Safeguards*.
Crisis	A critical event, which if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation or ability to operate.
Crisis Management	The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation or ability to operate.
Crisis Management Plan (CMP)	A document defining a communication method and management approach for providing timely, consistent and accurate crisis information to employees, customers and the public.
Cryptographic algorithm	A specific type of computational procedure that takes variable inputs, including a cryptographic key, and produces an output. Also called a *cipher*.

D

TERM	DEFINITION
Damage Assessment	The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.
Data Center Recovery	The component of *disaster recovery* which deals with the restoration, at an alternate location, of data center services and computer processing capabilities.
Data Loss	The unauthorized use and or transmission of confidential information. Typically refers to information leaving the control of the owning organization, for example on portable devices/media or via email. **Also Called:** Data Leakage
Data Loss Prevention (DLP)	Processes or automated systems designed to stop *data loss*.
Data Owner	A person in a senior leadership position of an organization that has financial accountability or legal liability for the data.
Declaration Fee	A one-time fee, charged by an Alternate Facility provider, to a customer who declares a disaster. **Similar Terms:** Notification Fee.
Dedicated Line	A pre-established point to point communication link between computer terminals and a computer processor, or between distributed processors, that does not require dial-up access.
Demilitarized Zone (DMZ)	A network between an organization's internal network and the public network (Internet) that hosts externally facing services such as web servers or email. **Also Known As:** Data Management Zone; Demarcation Zone
De-provisioning	*See Provisioning*
Dial Backup	The use of *dial-up lines* as a backup to dedicated lines.
Dial-Up Line	A communication link between computer terminals and a computer processor, which is established on demand by dialing a specific telephone number.
Digital Certificates	An electronic document that contains a set of data that uniquely identifies an entity that includes the subject's public key and

TERM	DEFINITION
	other identifying information about the subject. The certificate is digitally signed by a *Certification Authority* (CA) to bind the key and subject identification together. **Example:** An electronic equivalent of an ID card, used in public key cryptography to digitally sign and/or encrypt messages and documents.
Digital Signature	An electronic 'signature', using *digital certificates*, that authenticates the identity of the sender of a message or the signer of an electronic document, that ensures the original content of the message or document is unchanged.
Disaster	Any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time. **Similar Terms:** Business Interruption; Outage; Catastrophe; Emergency.
Disaster Prevention	Measures employed to prevent, detect, or contain incidents which, if unchecked, could result in disaster.
Disaster Recovery	The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.
Disaster Recovery Plan (DRP)	A document that defines the resources, actions, tasks and data required to recover information assets in the event of a business interruption. **Similar Terms:** Continuity of Operations Plan; Business Continuity Plan.
Disaster Recovery Planning	The advance planning and preparations that are necessary to minimize loss and ensure continuity of the critical technology functions of an organization in the event of disaster.
Distributed Processing	Use of computers at various locations, typically interconnected via communication links for the purpose of data access and/or transfer.

E

TERM	DEFINITION
Electronic Signature	See *Digital Signature*
Electronic Vaulting	Transfer of data to an offsite storage facility via a communication link rather than via portable media. Typically used for

TERM	DEFINITION
	batch/journaled updates to critical files to supplement full backups taken periodically.
Emergency	Any event which disables or interrupts the ability to maintain a "business as usual" environment for a period of time that adversely affects the mission of an organization and results in great damage or loss.
Emergency Preparedness	The discipline that ensures an organization, or community's readiness to respond to an emergency in a coordinated, timely, and effective manner.
Emergency Response Procedures	A plan of action to commence at the time of an incident to prevent the loss of life and minimize injury and property damage.
Essential Records	Records or documents, for legal, regulatory, or operational reasons, which if damaged or destroyed would impair the organization's ability to conduct business and/or require replacement or recreation at considerable expense.
Encrypt (-ed) (-ion)	A process of transforming information (called *plaintext*) using an *cryptographic algorithm* (called a *cipher*) to make it unintelligible information (called *ciphertext*) except to authorized users with special knowledge (called a *key*) to decrypt the information back into plaintext.
Enterprise Vulnerability Management System (EVMS)	The people, processes, and technology used to inventory IT assets, assess and prioritize vulnerabilities, remediate risks, and verify the remediation of those vulnerabilities.
Environmental Disaster	The effects of *environmental threats* that affect the environment and lead to large scale impact on the environment, economy, or human lives.
Environmental Threat	Human behavior that impacts the environment or the secondary impact of a *natural disaster*, which could cause an interruption in business functions for some predetermined period of time or the compromise of security controls. **Example:** Chemical, Biological, Mechanical **Example:** A chemical spill from an overturned train that causes an evacuation of an office building.
Ethernet	A common standard for connecting computers into a *local area network* (LAN).

TERM	DEFINITION
Event	An identifiable occurrence within an ongoing stream of monitored inputs (e.g., network traffic, error conditions, signals, etc.) that has significance for a system and typically represents some outcome in the form of a message, token, count, pattern, value, or other marker. **Example:** User generated events like keystrokes, mouse clicks, file access, etc.
Extra Expense Coverage	Insurance coverage for disaster-related expenses, which may be incurred until operations are fully recovered after a disaster.
Extranet	A network based on standardized *internet* protocols belonging to one (or more) organization(s) for conducting business and/or sharing information with business partners, vendors/suppliers, customers or other authorized individuals. An extranet's web sites look and act just like any other public internet web sites, but the security perimeters surrounding an extranet make it inaccessible to the general public. **See Also:** *Intranet*, *Internet*
	A Web site for customers rather than the general public; uses the public Internet as its transmission system, but requires passwords to gain entrance.

F

TERM	DEFINITION
False Positive	An indication or report that a condition is positive (or exists) when it actually isn't (doesn't). This term is often used in automated scanning operations, such as *Intrusion Detection*, where a false positive incorrectly indicates malicious activity is occurring.
False Negative	An indication or report that a condition is negative (or doesn't exist) when it actually is positive (does exist)
File Server	A *server* providing the service of file sharing.
Forensics	The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

TERM	DEFINITION
Forward Recovery	The process of recovering a data base to the point of failure by applying active journal or log data to the current backup files of the data base.
Function	An activity required to complete a *process*. *Services*, *processes*, and *functions* are the three activities performed by an agency to meet the mission of the agency as defined by state statute. A *service* is comprised of one or more *processes*, which are themselves composed of one or more *functions*.

G

TERM	DEFINITION
Government Data	All data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use. **Example:** Information submitted by a Minnesota citizen when applying for a drivers license. **Example:** An e-mail address submitted by some someone to a State run website in order to be included on an e-mail list.
Government Entity (ies)	Any office, department, division, bureau, board, commission, authority, district, or agency of Minnesota State Government, usually qualified by a specific branch or government level. **Example:** Department of Revenue is an Executive branch government entity **Example:** City of Minneapolis is a local government entity
Guideline	Non-mandatory, supplemental information about acceptable methods for implementing or for going beyond the minimum requirements found in *policies* and *standards*

H

TERM	DEFINITION
Hack (-er) (-ing)	Generally, a hacker is a person who breaks into or subverts information systems for notoriety, malicious/destructive intent, or personal gain. However, there are also connotations have a positive or ethical usage.

TERM	DEFINITION
Host (*-ing*)	1) An *information system* connected to a network that '*hosts*' information or provides services to other systems (typically known as *clients*). 2) A mainframe system 3) A service provider '*hosting' platforms* and services, such as application, database or web services
Hot Site	An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster. Hot-sites may vary in type of facilities offered (such as data processing, communication, or any other critical business functions needing duplication). Location and size of the hot-site will be proportional to the equipment and resources needed. **Similar Terms:** Backup site; Recovery site; Recovery Center; Alternate processing site.
Human Threats	Possible disruptions in operations or breach of security controls resulting from intentional or unintentional human actions.

I

TERM	DEFINITION
Identity	The collection of attributes, physical or electronic, that make up a unique instance of an item within a larger class of items. Identities are used, once *authenticated*, to *authorize* access to systems, information, physical locations, and many other types of resources and/or *privileges*. **Example:** physical identities such as badges, licenses, passports; electronic identities such as user accounts, email addresses, employee or social security numbers
Identification	The process of discovering or verifying an *identity*. In relation to electronic identities, verifying the presented *identity* is more accurately referred to as *authentication*.
Document Imaging	The process of converting paper records into digital copies or images.
Forensic Imaging	The process of creating an identical copy or replica of an electronic device (e.g. hard drive, *removable media*, portable memory), for the use in computer forensics.

TERM	DEFINITION
Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information (loss of *confidentiality*), unauthorized modification or destruction of information (loss of *integrity*), or disruption of access to or use of information or an information system (loss of *availability*).
Impact Ratings	A method of categorizing the level of *impact* to an *information system*. **High Impact**: The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic impact on the mission or core services of the entity, meaning, for example: priority services can not be delivered; major damage to assets or financial loss will occur; or the imminent threat of loss of life or serious life-threatening injuries exists. **Moderate Impact**: The loss of confidentiality, integrity, or availability could be expected to have a serious adverse impact on the mission, core services and/or supporting services of the entity, meaning, for example: significant degradation in service delivery is expected; significant damage to assets or financial loss will occur; or the potential for non-life-threatening injuries exists. **Low Impact**: The loss of confidentiality, integrity, or availability could be expected to have a limited adverse impact on the services of the entity, meaning, for example: limited degradation in service delivery impacting efficiency or effectiveness; minor damage to assets or limited financial loss; or minor harm to individuals.
Inactive	An identity (e.g. userid, badge), system, or other item that has not been actively used for a period of time and that may or may not still be valid/available for use. Through administrative action or automatic controls, inactive accounts, systems, etc may be disabled, made inactive, or otherwise invalidated for use pending further review and/or removal (de-provisioning). **Example: a *userid* which has not be utilized in 6 months may be,**

TERM	DEFINITION
	depending on policy, considered inactive and subject to removal
Incident	Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in the quality of that service. (ITIL perspective)
Incident Management Plan (IMP)	A document defining the structure, roles and responsibilities, process and procedures aimed to minimize the impact of a disruption to an agency by managing available resources of various disciplines.
Incident Response	The manual and automated procedures used to respond to reported incidents (real or suspected), systems failures and errors, and other undesirable events.
Information Asset(s)	Any information, regardless of its physical form, and the systems or processes used to manage that data.
Information System	Combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making. In other words, any combination of information technology and people's activities using that technology to support operations, management, and decision-making.
Information System Owner(s)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Integrity	The assurance that computerized data is an accurate and complete representation of the data as created or modified by its originator and that computerized information resources remain configured as intended by the person responsible for them.
ISO – International Organization for Standardization	The ISO works with standards institutes from over 150 countries to develop technology and product standards. The ISO is important to the computer industry, since the organization standardizes many of the technologies used by computer hardware and software.
Internet	A global system of interconnected computer networks that use standardized protocols to communicate. It is a 'network of networks', consisting of millions of private and public local and global networks in over 100 countries.
Internet Relay	A form of real-time internet text messaging, primarily used for

TERM	DEFINITION
Chat (IRC)	group discussions in forums called channels, but also allowing data transfer and one-to-one communication in private messages or chats..
Intranet	A network based on standardized *internet* protocols belonging to a single organization and accessible only by the organization's members, employees, or others with authorization. An intranet's web sites look and act just like any other public internet web sites, but the security perimeters surrounding an intranet make it inaccessible to the general public. **See Also:** *Extranet*, *Internet*
Intrinsic Value	The value of an asset to the business or government entity that is above and beyond its material or depreciated value.
Intrusion Detection	The process of detecting actions that attempt to compromise the *confidentiality*, *integrity* or *availability* of an *information asset*. It can be manual (e.g. log reviews) or automated with a toolset (see *Intrusion Detection System*).
Intrusion Detection System (IDS)	An automated system that performs *Intrusion Detection* activites, providing the capability to review larger quantities of data, generate reports and automated alerts as required. IDS has several variations: - network-based (inspects network traffic) or host-based (local to a single system, reviews local logs or activity) - signature-based (looks for known patterns of malicious activity) or anomaly based (looks for activity outside of an established 'normal' baseline).
IP Security (IPsec)	An Institute of Electrical and Electronic Engineers (IEEE) standard, Request For Comments (RFC) 2411, protocol that provides security capabilities at the Internet Protocol (IP) layer of communications. IPsec's key management protocol is used to negotiate the secret keys that protect Virtual Private Network (VPN) communications, and the level and type of security protections that will characterize the VPN. The most widely used key management protocol is the Internet Key Exchange (IKE) protocol.
Intrusion Prevention System (IPS)	An automated system similar to an *Intrusion Detection System* but with the capability to react in real-time to block or prevent malicious or unwanted activity.

TERM	DEFINITION
IT Auditor	CISO personnel, Agency Internal Auditors, or staff of a private firm that has the experience and expertise required to perform IT security audits without a conflict of interest.

J

TERM	DEFINITION

K

TERM	DEFINITION
Kerberos	A widely used authentication protocol developed at the Massachusetts Institute of Technology (MIT). In “classic” Kerberos, users share a secret password with a Key Distribution Center (KDC). The user, Alice, who wishes to communicate with another user, Bob, authenticates to the KDC and is furnished a “ticket” by the KDC to use to authenticate with Bob
Keystroke Logger	A program that records the keystrokes on a computer. It does this by monitoring a user's input and keeping a log of all keys that are pressed. The log may be saved to a file or even sent to another machine over a network or the Internet. Keylogger programs are often deemed spyware because they usually run without the user knowing it. They can be maliciously installed by hackers to spy on what a user is typing.
Key Management	The activities involving the handling of cryptographic keys and other related security parameters (e.g., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

L

TERM	DEFINITION
LAN Recovery	The component of Disaster Recovery which deals specifically with the replacement of LAN equipment in the event of a disaster, and the restoration of essential data and software.
Leased Line	Usually synonymous with *dedicated line*.
Least Privilege	The security objective of granting users only those accesses they need to perform their official duties..

TERM	DEFINITION
Likelihood	Determining the probability of a future event or circumstance based on the measure of past events or current state. Making an(a) inference, assumption, or distinction about the quality or complexity of future events or patterns based on the qualitative measure of past events.
Limited Remote Access	Individual and devices that have access to a limited set of resources and leverages additional controls to ensure the security of State data (e.g., SSL encrypted data transmission by application, additional authentication by application, etc.)
Line Rerouting	A service offered by many regional telephone companies allowing the computer center to quickly reroute the network of dedicated lines to a backup site.
Line Voltage Regulators	Also known as surge protectors. These protectors/regulators distribute electricity evenly.
Local Access	Physical or logical access, or connectivity, to remote processing capability using workspace or equipment at a local site. **Example:** 'Local Access Suite', which is a workspace recovery capability nearby to a primary work site allowing connectivity with remote mainframe or server(s)
Local Area Network (LAN)	Computing equipment, in close proximity to each other, connected through a wired or wireless network that does not utilize a public carrier.
Login	The process of presenting an identity (a *userid* typically) and *authentication* (a *password*, *token*, or other item) to gain access to information systems and resources.
Login ID	See *UserID*
Logon	See *Login*
Logon Banner	A message provided to an individual attempting to *login* to an information system, typically to outline *policies* related to use of the system.
Loss	The unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.
Loss Reduction	The technique of instituting mechanisms to lessen the exposure

TERM	DEFINITION
	to a particular risk. Loss reduction is intended to react to an event and limit its effect. Examples of Loss Reduction include sprinkler systems, insurance policies, and evacuation procedures.

M

TERM	DEFINITION
Malware	A program that is inserted into a system, usually covertly, with the intent of compromising the *confidentiality*, *integrity*, or *availability* of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Media	A general term referring to the material onto which business information has been recorded and may subsequently be used for business purposes. **Example**: Paper, microfiche, optical disc (CD/DVD/other), floppy disk, magnetic tape, memory card
Mitigate	To lessen in force or intensity. To mitigate a *vulnerability* is to take actions that reduce the vulnerability's impact or exposure.
Mitigating Control(s)	*Controls* utilized to *mitigate* the probability of a *risk* occurring. For further definition, SEE *Controls*
Mitigating Factor(s)	Any item that may reduce the probability of a *risk* occurring. This is a broader term than *mitigating controls*, representing also items the entity may not control or have to take action to carry out. **Example:** Not being in a flood plain is a *mitigating factor* against the risk of flood damage.
Mobile Hot-Site	A large trailer containing backup equipment and peripheral devices delivered to the scene of the disaster, which is then hooked up to existing communication lines.
Multi-factor Authentication	The use of two or more authentication factors to validate an *identity*. Authentication factors are pieces of information unique to an individual and are typically classified as: 1) something the user **has** (e.g. id card, token, certificate);

TERM	DEFINITION
	2) something the user **knows** (e.g. password, PIN, phrase or code); 3) something the user **is** (fingerprint, retinal pattern, voice print, signature, or other biometric identifier); 4) **somewhere** the user is (GPS coordinates, inside a controlled room) This is commonly refered to as *two-factor authentication*, because the general practice is to use two of the above four items to identify and authenticate a user. **Example:** requiring a: hardware token & PIN for remote access, fingerprint & password for logon, bank card & PIN for ATM

N

Term	Definition
Natural Disaster	The effects of *natural threats* that affect the environment and lead to large scale impact on the environment, economy, or human lives.
Natural Threats	Naturally occurring events that may cause disruptions to an organization or have other negative effect on people or the environment. Also known as 'Natural Hazard'. **Example:** Earthquake, wildfire, tornado, blizzard, flood
Need To Know	The security principle that describes additional restrictions on information such that, even if the necessary authorization to access a certain level of information is in place, access would not be given to sensitive information unless there is a specific 'need to know'. Discourages 'browsing' of highly sensitive information by limiting access to a minimum of people.
Network	A system of interconnected hardware, software and cabling (or radio, in wireless systems) that enables computers and other devices to communicate and exchange information (e.g. data, voice, video). Networks are often defined by scale or location, e.g. Local Area Network (LAN), Wide Area Network (WAN), Intranet/Extranet.
Network Access	A combination of policies and technology designed to validate

Term	Definition
Control	the integrity and/or authorization of information systems to connect to a computer network, thus preventing rouge, mis-configured or infected systems from endangering others on the network. Integrity often checks include, but are not limited to, ensuring the system utilizes updated anti-virus software, has a firewall, has software at expected patch levels, and/or runs only authorized software.
Network Address Translation (NAT)	The process of modifying network addresses while in transit across a network traffic routing device for the purpose of remapping a given address space into another.
Nonessential Function	Business activities or information which could be interrupted or unavailable indefinitely without significantly jeopardizing critical functions of an organization.
Nonessential Records	Records or documents which, if irretrievably lost or damaged, will not materially impair the organization's ability to conduct business.
Non-Repudiation	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Nonvolatile Memory	A general term for all forms of solid state (no moving parts) memory that do not need to have their memory contents periodically refreshed. This includes all forms of read-only memory (ROM) such as programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), electrically erasable programmable read-only memory (EEPROM), and flash memory. It also includes random access memory (RAM) that is powered by a battery
Not Public Data	Any data collected, created, maintained or disseminated by a state agency which has a classification other than public. This includes *confidential, private, nonpublic* or *protected nonpublic* data as those terms are defined in the Minnesota Governmental Data Practices Act or any other relevant state or federal statute.

O

TERM	DEFINITION

TERM	DEFINITION
Off-Host Processing	A backup mode of operation in which processing can continue throughout a network despite loss of communication with the mainframe computer.
Off-Line Processing	A backup mode of operation in which processing can continue manually or in batch mode if the on-line systems are unavailable.
Offsite	In another location. It is common practice to store copies of important data off site as part of a disaster recovery program. **Example: The records management program stores documents *offsite*.**
Off-Site Storage Facility	A secure location, remote from the primary location, at which backup hardware, software, data files, documents, equipment, or supplies are stored.
On-Line Systems	A computer system supporting users through their computing devices over a network.
Onsite	At the current location. **Example: Our primary system uses *onsite* processing and storage.**
Open System Interconnection Reference Model (OSI Model)	A framework for layered communications and computer network protocol design. The OSI model divides network architecture into seven layers to manage communication from the application level all the way down to physical media. Control passes directly from one layer to the next with each layer having unique *protocols* to communicate with the corresponding layer in another host.
Operating System (OS or O/S)	A software interface between hardware and users, in computers and most other electronic devices (phones, printers, scanners, etc.) . The operating system also acts as a host for other applications or software that run on the particular machine. **ALSO KNOWN AS**: Operating Software

P

TERM	DEFINITION
Patch	A small piece of software designed to fix problems with or update computer programs. The patch is an actual piece of object code that is inserted into (*patched* into) an executable program.

TERM	DEFINITION
Patch Management	The process of strategically planning the selection and deployment of *patches* across an organization.
Password	A secret word or string of characters that is used for *authentication*, to prove identity or gain access to a resource. The terms access code or pass code are sometimes used when the secret information is entirely numeric.
Password	A secret word or string of characters (letters, numbers or other symbols) that is used to *authenticate* an *identity*.
Password Complexity	A measure of how 'strong' a *password* is based upon the mixture of characters used to create it, with a short dictionary word, such as 'apple', considered a weak password and a long, non-dictionary word including numbers, symbols and mixed case, such as 'Get$2go0nTrip' considered much stronger.
Passphrase	A memorable sequence of words or other text used to control access to a computer system, program or data. It is similar to a *password* in usage but is usually longer and may contain blank spaces. **Example:** The following sentence would be used completely as the *passphrase*: 'My dream trip is to Paris'
Penetration Testing (*pen-testing*)	The security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit, which could include an exploration of the security features of the system in question, followed by an attempt to breach security and penetrate the system or network.
Perimeter Security	A *network* protection or defense design where security devices, such as *firewalls*, are positioned to inspect and interdict network traffic from external untrusted networks as it attempts to pass to internal protected networks.
Peripheral Equipment	Devices connected to a computer processor which perform such auxiliary functions as communications, data storage, printing, etc.
Permission(s)	An individual entry in an *Access Control List* on a resource (e.g. file, folder, share, printer, service) that define rights (e.g. Read, Write, Execute, Delete) that a user, or group of users, has to that resource. *Permissions* are attributes of a resource, versus *privileges*, which are attributes of a user and/or system.

TERM	DEFINITION
Personal Firewall	Software running on a computer that inspects network traffic passing through it and permits or denies passage based on a set of rules. See *firewall* for a description of a network device that protects larger segments of a *network*.
Phishing	Tricking individuals into disclosing sensitive personal information through deceptive computer-based means, such as through specially crafted emails.
Physical Safeguards	Physical measures taken to prevent a disaster, such as fire suppression systems, alarm systems, power backup and conditioning systems, access control systems, etc.
Physical security	The application of control procedures as measures to prevent or deter attackers from accessing a facility, resource, or information. It can include items such as physical barriers to gaining access, electronic security and alarm systems, video monitoring, staffed security or other response.
Plan Activation	The time at which all or a portion of the business continuation plan has been put into motion.
Plaintext	Information that has meaning and can be understood without the application of decryption. In *encryption*, *plaintext* is the data input to the Cipher or output from the Inverse Cipher.
Platforms	Hardware and/or software architecture that allows other software to run. **Example:** Platform often refers to hardware (e.g. IBM, Tandem, HP), operating system (e.g. Unix, Windows, Sun), software (Java, .NET) or some combination of each.
Policy	A senior leadership statement that indicates the direction or intent of an organizational propose for a given subject area.
Port	Hardware: A physical interface between a computer and other computers or devices (either external or internal to the computer). Software: A virtual data connection between computer programs used to exchange data.

TERM	DEFINITION
	Example: Hardware: Serial port, parallel port, PS/2; Software: TCP or UDP ports
Portable Computing Device	Laptop personal computers, tablet personal computers, personal digital assistants or other such devices capable of storing and processing data, and connecting to a network.
Portable Media	See *Removable Media*
Privileged Account	User accounts that been assigned special or elevated privileges, usually on a system-wide basis, as compared to normal user accounts **Example:** RACF 'Special'; Unix 'Superuser', Windows 'Domain Administrator'
Privilege	A special role or administrative duty that can be granted to users to perform specific management tasks within a computer system. *Privileges* are attributes of a user and/or system, versus *permissions*, which are attributes of a resource.
Procedural Safeguards	Procedural measures taken to prevent a disaster. **Example:** Safety inspections, fire drills, security awareness programs, records retention programs.
Process	A collection of business activities (*functions*) undertaken to complete a *service*. *Services*, *processes*, and *functions* are the three activities performed by an agency to meet the mission of the agency as defined by state statute. A *service* is comprised of one or more *processes*, which are themselves composed of one or more *functions*.
Provisioning	The process of allocating, adjusting and de-allocating user entitlements (e.g. *accounts, attributes, privileges, permissions)* based on defined business rules and security policies.

Q

TERM	DEFINITION
Qualitative	Expressible in terms of subjective quality or relative characteristics.
Quantitative	Expressible in terms of, or involving the measurement of, a quantity or amount.

R

TERM	DEFINITION
Reasonable measures	The minimum acceptable set of controls that an agency would be expected to have, given its industry, its location, the nature of its business, and other aspects of its situation; i.e., due diligence.
Reciprocal Agreement	An agreement between two organizations with compatible computer configurations allowing either organization to utilize the other's excess processing capacity in the event of a disaster.
Record(s)	Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
Records Management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of *records*, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the forms of records.
Record Retention	The process of retaining, *on-* or *offsite*, physical or electronic *records* for a period of time, as defined in a *Records Management* program, usually to comply with state and federal law and/or other mandated requirements or regulations.
Recovery Point Objective (RPO)	The point in time (referring to a point prior to an incident) to which data must be synchronously restored in order to resume processing transactions. RPO refers to the tolerance for the loss of data measured in terms of the time between the last backup of data and the disaster event.
Recovery Strategy	The method selected to recover the critical business functions following a disaster. In data processing, some possible alternatives would be manual processing, use of service bureaus, or a backup site (hot or cold-site). A recovery alternative is usually selected following either a Risk Analysis, Business Impact Analysis, or both.
Recovery Time Objective (RTO)	The maximum period of time available for recovering time sensitive processes before there is a significant impact on the agency.
Registration Authority (RA)	An organization responsible for maintaining lists of codes under international standards.
Remediate (-tion)	The act of correcting a vulnerability or eliminating a threat. **Example:** Three possible types of remediation are installing a

TERM	DEFINITION
	patch, adjusting configuration settings, or uninstalling a software application.
Remote	At a location other than the primary site.
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter. Access can be from a remote location or facility, or from within a local site but external to the particular resource accessed. **Example:** VPN access to an enterprise network; remote administrative console access to a system
Remote Channel Extension	Most commonly used to replace or consolidate mainframes, or to place peripherals in remote locations. By employing channel extenders, the input-output devices (such as terminals or printers) currently connected to a local computer can be connected to a remote computer.
Remote DASD Mirroring	A hardware solution for duplicating data on a disk to another disk. A standby database maintains a copy of a production database but in a permanent state of recovery. If the production database fails then the standby database can be opened (or promoted) with minimal recovery.
Remote Site	An alternate processing site that is equipped to provide recovery to a hot-site that is not located in the same geographical location.
Removable Media	Data storage devices or *media* that can be easily removed (i.e. are portable) from the reader device (e.g. disk drive, optical drive, USB port, hub/cradle). **Example:** USB flash drive, digital memory card, CD/DVD, floppy disks, ZIP disks, external hard drive
Residual Risk	The remaining, potential risk after all IT security measures are applied. There is a residual risk associated with each threat.
Retention Period	An attribute of a *record* that represents the period of time a document should be kept by an organization to comply with applicable mandates, as defined within a *Records Management* program.
Risk	A measure of the exposure to which an organization may be subjected. This is a combination of the likelihood of a threat exploiting a vulnerability, causing a business disruption, and the possible impact or loss that may result from the business disruption.

TERM	DEFINITION
	Risk = (probability of event occurring) x (impact of event occurring) The four common ways to treat risk are: • *Risk avoidance*: stop activity with risk(s) • *Risk reduction*: *mitigate* or *remediate* risk(s) • *Risk transfer:* move risk(s) to another body, such as buying insurance or outsourcing • *Risk acceptance*: retaining some (*residual risk*) or all of the risk(s)
Risk Acceptance	The formal acceptance of all remaining *residual risk*.
Risk Assessment	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management and incorporates threat and vulnerability analyses. **Similar Terms:** Risk Analysis; Impact Assessment; Corporate Loss Analysis; Risk Identification; Exposure Analysis; Exposure Assessment.
Risk Assumption	See *Risk Retention.*
Risk Avoidance	A method of mitigating risk by choosing not to perform the activity associated with the risk. However, this also means the potential gains are also not realized.
Risk Communication	The exchange or sharing of information about risk between the decision-maker and other stakeholders
Risk Estimation	The process to assign values to the probability and consequences of a risk.
Risk Exposure	The total risk to a system or entity from a specific vulnerability or set of vulnerabilities.
Risk Management	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; the formal authorization to operate the system or process; and employment of techniques and procedures for continuous monitoring of the

TERM	DEFINITION
	system or process. Risk Management considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Risk Mitigation	The process of prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the *risk assessment* process.
Risk Retention	A method of dealing with risk in an activity by choosing to accept the impact of the risk, or any *residual risk*, should it actually occur. SEE *Risk Acceptance*.
Risk Reduction	The actions taken to lessen the probability or consequences, or both, associated with a risk.
Risk Threshold	See *Risk Tolerance*.
Risk Tolerance	The degree of *residual risk* an entity is willing to accept. **Also Known As:** Risk Appetite
Risk Transference	A method of dealing with risk by choosing to move the activity with risk to another entity. **Example:** Purchasing insurance against an event; outsourcing activities with unacceptable risks
Role Based Access Control (RBAC)	An approach to securing access to resources based on the role(s), or job function(s), a user fills in an organization. In RBAC, permissions to resources are assigned to roles, not directly to users. Users acquire (or lose) access when they fill (or leave) a particular role, greatly simplifying provisioning of access.
Rootkit	A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.

S

TERM	DEFINITION
Safeguard(s)	Protective measures prescribed to meet the security

TERM	DEFINITION
	requirements (i.e., *confidentiality*, *integrity*, and *availability*) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Salvage & Restoration	The process of reclaiming or refurbishing computer hardware, vital records, office facilities, etc. following a disaster.
Salvage Procedures	Specified procedures to be activated if equipment or a facility should suffer any destruction.
Sandbox(-ing)	A method of isolating application modules into distinct fault domains enforced by software. This technique allows untrusted programs to be executed safely within the single virtual address space of an application.
Sanitization	The removal of data so that it is unrecoverable from a given media form to a level commensurate with the sensitivity of the information.
Security	The practice of reducing the risk of and the degree of protection against threats exploiting vulnerabilities that could cause an undesirable result (e.g., theft, espionage, sabotage, danger, injury, information breach, etc.)
Security Assessment	The process of identifying technical computer/network/system security vulnerabilities, as well as weaknesses in policies and practices related to the operation of an information system.
Security Audit	A formal, in-depth *audit* of security directives and controls.
Security Authorization	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the *risk* to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Security Awareness	The extent to which every member of an organization understands: security and the levels of security appropriate to the organization; the importance of security and consequences of a lack of security; their individual responsibilities regarding security.
Security	A clearly and formally defined plan, structured approach, and set

TERM	DEFINITION
Awareness Program	of related activities and procedures with the objective of realizing and maintaining a security- aware organizational culture
Security Category	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Event	A notification of logged or reported *event*(s) that is/are suspected to be a *security incident,* but has not been validated.
Security Incident	A *incident* or *security event* that has been validated to be a violation of policy, has had an adverse effect on information assets or the delivery of services, or is a *threat* to health and safety.
Security Objectives	*Confidentiality*, *integrity*, or *availability* (CIA). **Also Known As:** Security Triad
Security Perimeter	The boundary that defines the area of security concern and security policy coverage.
Security Policy	A senior leadership directive that indicates the direction or intent of its established goals, and assign responsibilities for, addressing security risks to an organization.
Security Procedure	The formal documentation of specific operational steps and processes that specify how security goals and objectives set forward in the *security policy* and *security standards* are to be achieved.
Security Service	A capability that supports one, or many, of the security goals. **Example:** key management, access control, authentication
Security Standards	Practices, directives, guidelines, principles or baselines that state what needs to be done and focus on areas of current relevance and concern. They are a translation of issues already mentioned in the security policy.
Security System	The hardware, software, and processes required to secure the

TERM	DEFINITION
	information and telecommunication technology systems and services of the executive branch of Minnesota State Government.
Segregation of Duties	SEE *Separation of Duties*
Separation of Duties	A key concept of internal control that specifies having more than one person to complete a task, thereby reducing the risk of fraud or damage to the organization. **Example:** the person who creates purchase orders is not also the person who approves or pays them; the person who administers a system is not also the person who monitors the audit logs of the system
Service	The means by which an organization fulfills its mission. *Services*, *processes*, and *functions* are the three activities performed by an agency to meet the mission of the agency as defined by state statute. A *service* is comprised of one or more *processes*, which are themselves composed of one or more *functions*.
Service Accounts	A specific type of *userid* designed to be used by *information system* services, programming or other automated processes. These accounts are typically not accessed directly by users, but may be be used programmatically on a user's behalf.
Service Bureau	A data processing utility that provides processing capability, normally for specialized processing, such as payroll.
Server	An *information system* connected to a network that hosts information or provides services to other systems (typically known as *clients*). **Example:** file server, web server, email server, application server, database server
Shadow Database	An approach to data backup in which real-time duplicates of critical files are maintained at a remote processing site.
Shared Secret	A secret used in authentication that is known to the claimant and the verifier.
Simulation Test	A test of recovery procedures under conditions approximating a specific disaster scenario. This may involve designated units of the organization actually ceasing normal operations while exercising their procedures.

TERM	DEFINITION
Sniffer	Software that observes and records network traffic.
Social Engineering	An attempt to trick someone into revealing confidential or sensitive information (e.g., password, user account, account number) that can be used to attack systems or networks.
Software	Applications and services such as operating systems, database applications, networking software, office applications, custom applications, etc. that process, store, or transmit *government data*.
Spam	E-mail that is not requested. Also known as "unsolicited commercial e-mail" (UCE), "unsolicited bulk e-mail" (UBE), "gray mail" and just plain "junk mail," the term is both a noun (the e-mail message) and a verb (to send it).
Spoofing	Faking the sending address of a transmission in order to gain illegal entry into a secure system **Example:** "IP spoofing" (or "email spoofing") refers to sending a network packet (or email) with header information that makes it appear to come from a source other than its actual source.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Stand-Alone Processing	Processing, typically on a PC or mid-range computer, which does not require any communication link with a mainframe or other processor.
Standby Database	Maintains a copy of a production database but in a permanent state of recovery. If the production database fails then the standby database can be opened (or promoted) with minimal recovery.
State Agency	**See** *Government Entity*
State Data	**See** *Government Data*
Storage Media	Any device that can store (temporarily or permanently) data in an electronic format. **Example:** Hard Drives, CD's, DVD's, Thumb Drives, Floppy Disks, Tape Backups, *Volatile and Non-Volatile Memory*, Cell Phones, Handheld Devices, printers and copiers
Subnet	A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all

TERM	DEFINITION
	devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons.
Supporting Services	*Services* performed by an agency solely to support the execution of other agency *services*. Support services are usually provided organization-wide. **Example:** Purchasing, Internal Audit, Communications, Technology
System (-*s*)	"Information and telecommunication systems and services" as defined by state statute 16E.03, Subdivision 1(a), that process, store, or display *Government Data* that is a combination of software, hardware and any host, client or server.
System Categorization	SEE *Security Category*.
System Owner	SEE *Information System Owner.*
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

T

TERM	DEFINITION
Table Top Exercise	A test of recovery procedures in which team members walk through the plan to identify and correct weaknesses.
Technical Threat	A disaster-causing event that may occur regardless of any human elements.
Tempest	A name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.
Temporary Operating Procedures	Manual or automated procedures used in a disaster until normal operations can be restored.
Terminal Security	A method of securing resources based on location (virtual or physical) of the requesting system. Access to resources is

TERM	DEFINITION
	approved/disapproved based on 'where' the request for access originated from, independent from, or in addition to, user/group based security controls on the resource.
Test Plan	The recovery plans and procedures that are used in a systems test to ensure viability. A test plan is designed to exercise specific action tasks and procedures that would be encountered in a real disaster.
Threat	A natural, human, or environmental source with the intent or opportunity to trigger the exploitation of a vulnerability.
Threat Agent	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.
Threat Analysis	See *Threat Assessment*.
Threat Assessment	Formal evaluation and description of the type, scope and nature of events or actions that can result in adverse consequences to an organization or specific assets.
Threat Model (-ing)	The definition of a set of possible attacks against an information asset or other resource, to be used in assessing probabilities and prioritizing response.
Threat Source	See *Threat Agent*.
Threat Vector	The path or method utilized by a *threat*.
Time Stamp	The value of an object (e.g. event log) that indicates the system time at some critical point in the object's history (e.g. when a critical event happened).
Token	Something that the claimant possesses and controls (typically a key or password) used to authenticate the claimant's identity.
Topology	The physical or logical mapping of the location of networking components or nodes within a network.
Trojan Horse	Purposefully hidden malicious or damaging code within an authorized computer program. Unlike viruses, trojans do not replicate themselves.
Two Factor Authentication	See *Multifactor Authentication*

U

TERM	DEFINITION
Unique Identifier (UID)	An integer value that uniquely identifies users in Unix-like systems. Also known as 'user identifier'. See Also: Group Identifier (GID)
User(s)	An individual, or (system) process on behalf of an individual, that is authorized to access an information system.
UserID	The *account* within an information system that is used to *identify* a user. **Also Known As:** User Account, Username, Login/on ID, Screenname
User Contingency Procedures	Manual procedures to be implemented during a computer system outage. **Similar Terms:** Temporary Operating Procedures.

V

TERM	DEFINITION
Virus	A parasitic software program, equipped with the means of reproducing itself, that when executed, spreads throughout a computer or network by attaching itself to or infecting (modifying) other software or diskettes.
Voice Recovery	The restoration of an organization's voice communications system.
Volatile Memory	A general term for all form of solid state (no moving parts) memory that do have their memory contents periodically refreshed or lost when power is interrupted. This is primarily referred to as random access memory (RAM) that is not powered by a battery.
Vulnerability	A flaw or weakness in a process, design, implementation, control, system, or organization that could be triggered or intentionally exploited, resulting in a *security incident* or breach.
Vulnerability Impact	The score produced by the vulnerability scanning system.
Vulnerability Management	A security practice designed to identify, track, and mitigate vulnerabilities in order to minimize the risk of the exploitation of

TERM	DEFINITION
	those vulnerabilities.
Vulnerability Scanning	An automated process that looks for known vulnerabilities within information systems, applications and/or networks.

W

TERM	DEFINITION
Warm Site	An alternate processing site which is only partially equipped (as compared to Hot Site which is fully equipped).
Wide Area Network (WAN)	Like a LAN, except that parts of a WAN are geographically dispersed, possibly in different cities or even on different continents. Public carriers like the telephone company are included in most WANs; a very large one might have its own satellite stations or microwave towers.
Wireless	In the broadest sense, it is the transfer of information over a distance without the use of wires. Commonly refers to connectivity of computing devices to networks over wireless networks.
Worm	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

X

TERM	DEFINITION	SOURCE
X.509	A widely used standard for defining digital certificates.	Webopedia

Y

TERM	DEFINITION	SOURCE

Z

TERM	DEFINITION	SOURCE
Zero Day Exploit	A zero day exploit is a malicious computer attack that takes advantage of a security hole before the vulnerability is known. This means the security	TechTerms

TERM	DEFINITION	SOURCE
	issue is made known the same day as the computer attack is released. In other words, the software developer has zero days to prepare for the security breach and must work as quickly as possible to develop a patch or update that fixes the problem.	
Zones	A zone file is stored on a name server and provides information about one or more domain names. Each zone file contains a list of DNS records with mappings between domain names and IP addresses. These records define the IP address of a domain name, the reverse lookup of an IP to other domains, and contain DNS and mail server information.	TechTerms

History & Ownership

Revision History – record additions as Major releases, edits/corrections as Minor

Date	Author	Description	Major #	Minor #
08/05/2009	Eric Breece	Initial Release	1	00
02/01/2011	Eric Breece	Addition of COOP terms and definitions	1	01

Review History – periodic reviews to ensure compliance with program

Date	Reviewer	Description	Compliance

Approval History – record of approval phases

Phase	Description	Date
SME	Enterprise Security Office	10/15/2010
ISC	Information Security Council Approval	N/A
CIOC	CIO Council Approval	N/A
CAB	Commissioners' Advisory Board Approval	N/A

Ownership – current owners of the document

	Owner	Division	Department
Primary	Chris Buse	Enterprise Security Office (ESO)	Governance
Secondary	Eric Breece	Enterprise Security Office (ESO)	Governance